

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
4 October 2001 (04.10.2001)

PCT

(10) International Publication Number  
WO 01/73530 A2

(51) International Patent Classification<sup>7</sup>: G06F 1/00

(21) International Application Number: PCT/US01/09631

(22) International Filing Date: 26 March 2001 (26.03.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:  
09/536,203 27 March 2000 (27.03.2000) US

(71) Applicant: SECURIT-E-DOC, INC. [US/US]; 1689 Forum Place, West Palm Beach, FL 33401 (US).

(72) Inventor: BARRON, Robert, H.; 1025 Morse Blvd., Singer Island, FL 33404 (US).

(74) Agent: SLAVIN, Michael; McHale & Slavin, P.A., 4440 PGA Blvd., Suite 402, Palm Beach Gardens, FL 33410 (US).

(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

**Published:**

— without international search report and to be republished upon receipt of that report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.



WO 01/73530 A2

(54) Title: METHOD, APPARATUS, AND SYSTEM FOR SECURE DATA TRANSPORT

(57) Abstract: A platform allowing for the secure file transfer from one location to another (internet or intranet) with virtually impregnable encryption, secure data storage, and a simple web-based user interface. A user accesses the system by a data-base authentication system requiring user name and password. The program residing on the server then generates an encryption sequence. A temporary file is created on the users' machine upon which the user uploads the information to be sent. The information is automatically encrypted by the program and transferred to the server and the user's temporary file deleted. The information is securely stored in the program on the server until the recipient downloads it. The recipient also accesses the server by a user name and password. The program generates a decryption program. The recipients machine receives the applet program to decrypt the file and a copy of the encrypted file. After decryption is complete, the program saves the files to a specified recipient folder, and can be automatically deleted or archived.

-2-

1           The interconnected computers exchange information  
2 using various services, for example, the World Wide Web  
3 (WWW) and electronic mail. The WWW created a way for  
4 computers in various locations to display text that  
5 contained links to other files. The WWW service allows a  
6 server computer system (Web server or Web site) to send  
7 graphical Web pages of information to a remote client  
8 computer system. The remote client computer system can  
9 then display the Web pages.

10           In a standard e-mail system, a user's computer is  
11 connected to a provider of Internet services, and the  
12 user's computer provides an e-mail password when polling  
13 the provider's computer for new mail. The mail resides on  
14 the provider's computer in plain text form where it can be  
15 read by anyone. In both examples, the information, if  
16 unsecured, is replicated at many sites in the process of  
17 being transmitted to a destination site and thereby is  
18 made available to the public.

19           Organizations are increasingly utilizing these  
20 networks, to improve customer service and streamline  
21 business communication through applications such as e-  
22 mail, messaging, remote access, intranet based  
23 applications, on-line support and supply chain  
24 applications. The very openness and accessibility that  
25 has stimulated the use of public and private networks has  
26 also driven the need for network security.

27           Presently, to provide for a secure transfer of  
28 information, it may be encrypted at the sending host's end  
29 and decrypted at the receiver's end. Encryption  
30 algorithms transform written words and other kinds of  
31 messages so that they are unintelligible to unauthorized  
32 recipients. An authorized recipient can then transform  
33 the words or messages back into a message that is  
34 perfectly understandable. Currently, there are two basic  
35 kinds of encryption algorithms (1) symmetric key

1 encryption keys from passphrases. For example, Pretty  
2 Good Privacy (PGP) uses message digests to transform a  
3 passphrase provided by a user in to an encryption key that  
4 is used for symmetric encryption. (PGP uses symmetric  
5 encryption for its "conventional encryption" function as  
6 well as to encrypt the user's private key). A few digest  
7 in use are HMAC, MD2, MD4, MD5, SHA, and SHA-1.

8 Working cryptographic systems can be divided into two  
9 categories; (1) programs and protocols that are used for  
10 encryption of e-mail messages such as PGP and S/MIME and  
11 (2) cryptographic systems used for providing  
12 confidentiality, authentication, integrity, and  
13 nonrepudiation in a network environment. The latter  
14 requires real-time interplay between a client and a server  
15 to work properly. Examples include Secure Socket Layer  
16 (SSL) a general-purpose cryptographic protocol that can be  
17 used with any TCP/IP service and PCT a transport layer  
18 security protocol for use with TCP/IP service, PCT, S-  
19 HTTP, SET, Cybercash, DNSSEC, Ipsec, IPv6, Kerberos, and  
20 SSH.

21 Although the present means of securing the electric  
22 transfer of information provides a level of security, the  
23 security provided can be easily breached. Symmetric  
24 encryption algorithms are vulnerable to attack by (1) key  
25 search or brute force attacks, (2) cryptanalysis, and (3)  
26 systems-based attacks. First, in a key search, the cracker  
27 simply tries every possible key, one after another, until  
28 the he/she is allowed into the system or the ciphertext is  
29 decrypted. There is no way to defend against this but a  
30 128 bit key is highly resistant because of the large  
31 number of possible keys to be tried.

32 Second, in cryptanalysis, the algorithm can be  
33 defeated by using a combination of sophisticated  
34 mathematics and computer power. Many encrypted messages  
35 can be deciphered without knowing the key. Finally, the

1 apparatus for encrypting data with a either a random  
2 automatic mode of encryption, and a client selected  
3 private key, that does not travel with the document. The  
4 method and apparatus, writes the encryption algorithm  
5 creating a packaged application. The encryption program  
6 generates random sequences or encryption algorithms, with  
7 respect to time sensitivity, to be used in the packaged  
8 application that it creates. No two algorithms will ever  
9 be the same.

10 In the basic embodiment, the client accesses the  
11 server using a data-base authentication system requiring  
12 User name and Password. Once access is granted, the  
13 packaged application is sent to the client machine as a  
14 temporary file to encrypt the files being sent or uploaded  
15 to the server. The application package breaks the files  
16 down into binary form, reads the binary form, and then  
17 rewrites the data to the temporary file it created. On a  
18 binary level, the code is rewritten and saved for transfer  
19 in a file format only decodable by the end recipient.  
20 Once this process is complete, the application packet then  
21 sends the encrypted data to the server via SSL protocol  
22 connection.

23 The data resides on the server waiting for an  
24 intended recipient to download and unlock it. When file  
25 retrieval is requested, the server authenticates the user  
26 and password via a log-on system. Once access is granted,  
27 the server generates a new application packet designed to  
28 decrypt the file being requested, based on the original  
29 encryption algorithm. The server retrieves its original  
30 entry, sets into motion the sequence of creating a  
31 decryption program, saves the generated program, and then  
32 sends the application packet to the requesting client  
33 machine.

34 The client machine receives the application packet to  
35 decrypt the file from the server and a copy of the file to

1 finger print scanner, smart card reader or the like and be  
2 implemented in order to send or retrieve information.

3 Yet another objective of the instant invention is to  
4 provide virtually impregnable security for the delivery,  
5 storage, and sharing of documents and files utilizing any  
6 compatible network as a secure communications forum.

7 Other objects and advantages of this invention will  
8 become apparent from the following description taken in  
9 conjunction with the accompanying drawings wherein are set  
10 forth, by way of illustration and example, certain  
11 embodiments of this invention. The drawings constitute a  
12 part of this specification and include exemplary  
13 embodiments of the present invention and illustrate  
14 various objects and features thereof.

15

16 BRIEF DESCRIPTION OF THE FIGURES

17 Figure 1 is a block diagram of the client file  
18 encryption transfer request of the instant invention;

19 Figure 2 is a block diagram of the encryption  
20 transfer;

21 Figure 3 is a block diagram of the recipient file  
22 request; and

23 Figure 4 is a block diagram of the decryption  
24 transfer.

25

26 DETAILED DESCRIPTION OF THE INVENTION

27 Although the invention will be described in terms of  
28 a specific embodiment, it will be readily apparent to  
29 those skilled in this art that various modifications,  
30 rearrangements, and substitutions can be made without  
31 departing from the spirit of the invention. The scope of  
32 the invention is defined by the claims appended hereto.

33 Now, referring to Fig. 1, shown is flow chart  
34 depicting the steps required for encrypting data allowing  
35 for secure transfer of electronic data. A client 10 opens

-10-

1 generated sequence specified by the particular and  
2 customized applet. The sequence is also designed to  
3 replace every other matching bit of binary code with a  
4 unique string. Thus, with this method, an "a", for  
5 example, will never be represented twice in the same file  
6 structure. This is designed to deter the common method of  
7 cracking encrypted code by repeated or pattern data. On  
8 a binary level, the code is rewritten and saved for  
9 transfer in a file format only decodable by the recipient.  
10 The applet then sends the encrypted data to the server via  
11 SSL protocol. Once the transfer is complete, the applet  
12 deletes any trace of the file encrypted. With the  
13 destruction of the applet, no two applications are ever  
14 the same because each application contains it's own  
15 encryption sequence that cannot be replicated.

16 The encrypted data resides on the server **12** waiting  
17 for an intended recipient to download and unlock it. This  
18 creates the ability to maintain completely encrypted and  
19 secure data archives. When file retrieval is requested by  
20 a recipient, the server then accesses the original record  
21 information of the sequence or algorithm that it  
22 originally gave to the applet that the server created to  
23 encrypt the file.

24 Now referring to Fig. 3, shown is the flow chart  
25 depicting the steps for decrypting data for a secure  
26 receipt of electronic data. A recipient **50** opens a web  
27 browser and accesses a qualified server **12** therein  
28 requesting data transfer. The server **12** provides login  
29 account qualifier data requiring either user name and a  
30 password **52** or a biometric interface **54** such as a retinal  
31 scanner, finger print scanner, smart card reader and the  
32 like for the purpose of seeking data-base authentication  
33 **56**. If login fails, the user has three attempts **58**  
34 before the account is locked **60** and the administrator and  
35 the account holder **62** is alerted.

-12-

CLAIMS1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35

What is claimed is:

Claim 1. A method of encrypting data for secure transfer and storage of electronic data comprising the steps of:

- accessing a conventional web browser;
- logging onto a qualified server and providing account qualifier data;
- reading a transfer information inquiry page upon verification of account qualifier;
- obtaining a first applet compiled on said server in response to said inquiry page, said first applet used to create a temporary file for the upload of data;
- submitting a file for encryption to said applet;
- encrypting said file and forming an encrypted data packet;
- forwarding said data packet to said qualified server for storage;
- providing a means for decrypting said encrypted data packet.

Claim 2. The method according to claim 1 wherein said account qualifier is a user name and password.

Claim 3. The method according to claim 1 wherein said account qualifier is a smart card reader.

Claim 4. The method according to claim 1 wherein said account qualifier is a biometric interface.

Claim 5. The method according to claim 4 wherein said biometric interface is a retinal scanner.

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35

Claim 13. The method according to claim 1 wherein said account qualifier is compared against a stored database.

Claim 14. The method according to claim 1 said encrypting of said file occurs during a transfer to said server.

Claim 15. A method of encrypting data for secure transfer and storage of electronic data comprising the steps of:

accessing a conventional web browser;  
logging onto a qualified server and providing account qualifier data;  
reading a transfer information inquiry page upon verification of account qualifier;  
obtaining a first applet compiled on said server in response to said inquiry page, said first applet used to create a temporary file for the upload of data;  
submitting a file for encryption to said applet;  
encrypting said file and forming an encrypted data packet;  
forwarding said data packet to said qualified server for storage and destroying said first applet;  
obtaining a second applet compiled on said server in response to said inquiry page, said second applet used to create a temporary file for the download of said encrypted data;  
decrypting said file and destroying said second applet.

Claim 16. The method according to claim 15 wherein said account qualifier is a user name and password.



-16-

1     decrypt said data file, said second applet allowing for  
2     the downloading and decryption of said data file.

3

4             Claim 25. The system according to claim 24, wherein  
5     said applets are controlled by a user name and password.

6

7             Claim 26. The system according to claim 24, wherein  
8     said sender selects a secondary private key to layer said  
9     encryption.

10

11            Claim 27. The system according to claim 26, wherein  
12     said secondary key is a digital file lock.

13

14            Claim 28. The system according to claim 26, wherein  
15     said secondary key biometric interface.

16

17            Claim 29. The system according to claim 24 wherein  
18     the recipient is notified of an encrypted data file by an  
19     e-mail message generated by said system and directed to  
20     said recipient.

21

22            Claim 30. The system according to claim 29 wherein  
23     said e-mail is sent by SSL protocol.

24

25

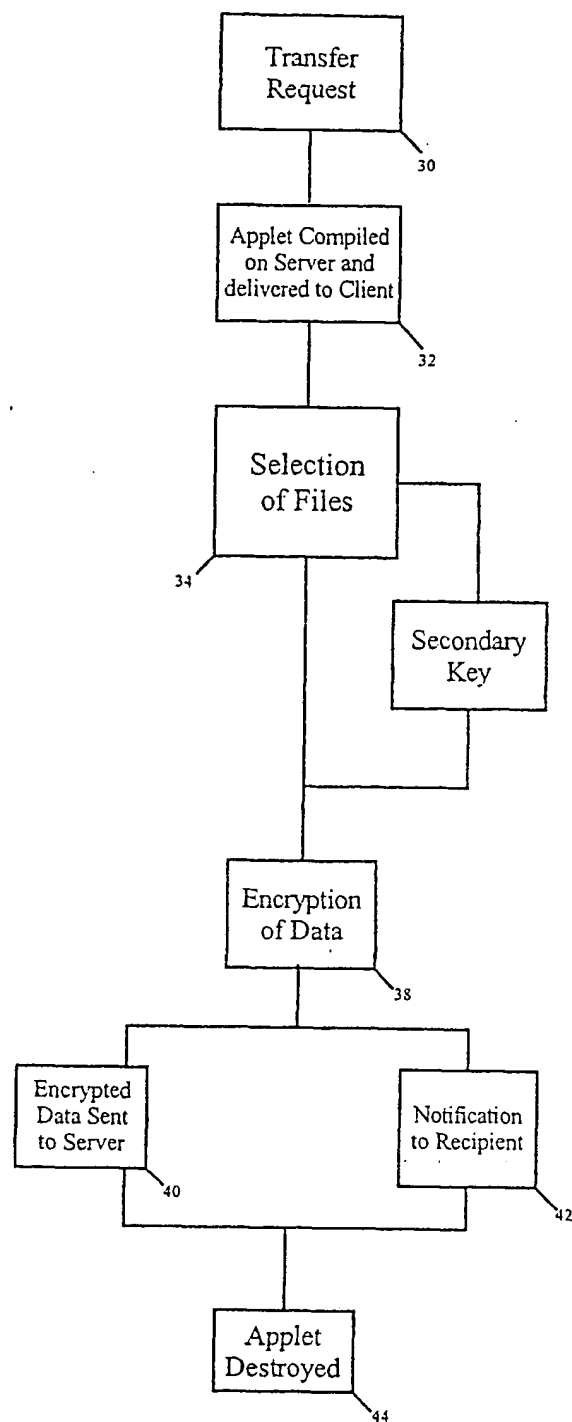


Fig 2

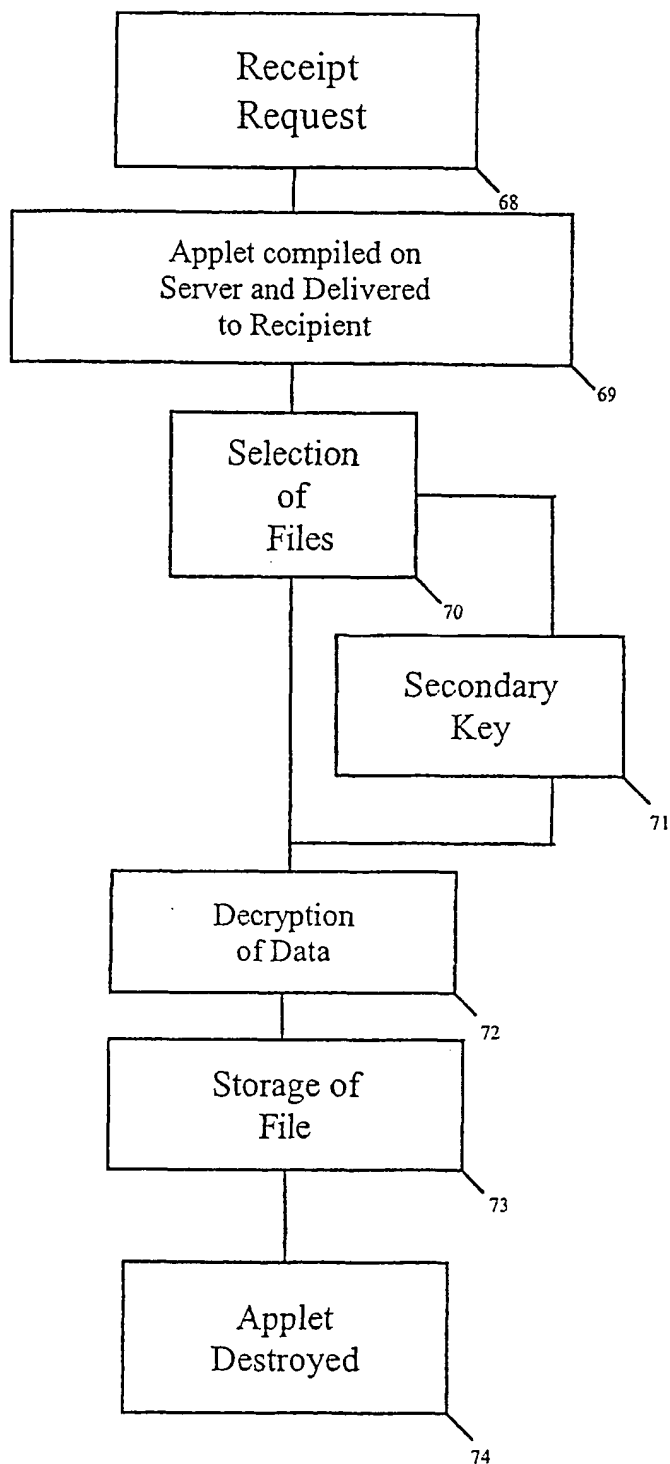


Fig 4.